

3

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-312364

(43)Date of publication of application : 09.11.1999

(51)Int.Cl.

G11B 20/10

H04N 5/765

H04N 5/781

H04N 5/92

H04N 7/24

(21)Application number : 10-118924

(71)Applicant : MITSUBISHI ELECTRIC CORP

(22)Date of filing :

28.04.1998

(72)Inventor : SEGI SHINICHI

(54) DIGITAL DATA RECORDING DEVIDEDIGITAL DATA REPRODUCING
DEVICEAND CHECK CODE GENERATING METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a digital data recording/reproducing device which can easily detect whether digital data recording in a medium is changed or not.
SOLUTION: Video inputted from a camera 2 is converted to digital video data by a video decoder 3and compressed to JPEG data by a JPEG compression/expansion means 4. Data is sampled from the JPEG data by a check code adding analyzer 12sampling data of 10 items are obtainedfurthera check code is generated by operating this sampling dataand added in the header of the JPEG data. The JPEG data with a check code thus generated is recorded in a recording medium 7. After thateven if recorded video data are altered by some oneit can be detected whether data is altered or not with high accuracy at the time of reproduction.

CLAIMS

[Claim(s)]

[Claim 1]A digital data recording device which records digital data on a recording mediumcomprising:

A data compression means which compresses digital data.

An extraction means to extract some data from compressed digital data based on the 1st code function.

A creating means which generates a check code based on the 2nd code function by making extracted data into a variable.

An addition means which adds said check code to a prescribed position of said compressed digital data.

[Claim 2]The digital data recording device according to claim 1 wherein said 2nd code function makes a variable a password which made a sampling number a variable.

[Claim 3]The digital data recording device according to claim 1 or 2 having had a JPEG compression means for said digital data to have been digital image data and to compress this digital image data and adding said check code in a header of JPEG compression data.

[Claim 4]Digital data playback equipment which reproduces digital data compressed and recorded on a recording medium comprising:

The 1st extraction means that extracts some data from compression digital data based on the 1st code function.

A creating means which generates the 1st check code based on the 2nd code function by making into a variable data extracted by said 1st extraction means.

The 2nd extraction means that extracts the 2nd check code added to compression digital data.

A comparison means to compare said 1st check code with said 2nd check code.

An extension means which elongates said compression digital data.

[Claim 5]Digital data playback equipment which reproduces digital data compressed and recorded on a recording medium comprising:

The 1st extraction means that extracts some data from compression digital data based on the 1st code function.

The 2nd extraction means that extracts a check code added to compression digital data.

A calculating means which calculates data extracted by said 1st extraction means and said check code based on the 3rd code function.

An extension means which elongates said compression digital data.

[Claim 6]The digital data playback equipment according to claim 4 or 5 having had a JPEG extension means which said digital data is digital image data and elongates compressed digital image data and extracting said check code from a header of JPEG compression data.

[Claim 7]It is a generation method of a check code used for digital data playback equipment of either a digital data recording device of either claim 1 thru/or claim 3 or claim 4 thru/or claim 6 A check code generation method extracting two or more sampling data out of compressed digital data and generating a check code by making a password which made a variable said extracted sampling data and its sampling number

into a variable.

[Claim 8]The check code generation method according to claim 7wherein a password which made said sampling number a variable is generated based on a code function.

[Claim 9]The check code generation method according to claim 7wherein said check code is generated by arithmetic addition function which makes extracted sampling data and said password a variable.

[Claim 10]The check code generation method according to claim 7wherein said check code is generated by addition on the Galois field which makes extracted sampling data and said password a variable.

[Claim 11]The check code generation method according to claim 7wherein said check code is generated by EXCLUSIVE OR operation which makes extracted sampling data and said password a variable.

[Claim 12]The check code generation method according to any one of claims 7 to 11wherein said sampling data are extracted based on a code function out of compressed digital data.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention]This invention relates to the generation method of the check code for detecting change of the digital image of the digital data record / playback equipment which records the compressed digital data on a recording mediumor is reproduced from a recording mediumand digital data record / playback equipment.

[0002]

[Description of the Prior Art]Drawing 8 is a block diagram showing the composition of the conventional digital image recording and reproducing device. The video camera by which 1 was connected to the digital image recording and reproducing deviceand 2 was connected to the digital image recording and reproducing device 1The video decoder from which 3 changes the analog video signal from the video camera 2 into a digital video dataCPU by which 4 performs a JPEG compression extension means and 5 controls this digital image recording and reproducing device 1The buffer memory used for temporary storing etc. of the JPEG data which 51 was connected to the data bus of CPU5and 6 was connected to the data bus 51and was compressed by the JrhoEG compression extension means 4archive mediasuch as etaDD for 7 to save JPEG dataand 9 -- the digital video data (Y.) of 4:2:2 profiles CRthe video encoder from which the data volume of CB changes the digital video data of 4:2:2 into an NTSC analog signaland 11 are the monitor TVs connected to the digital image recording and reproducing device 1.

[0003]The operation which records next the digital data compressed with this digital

image recording and reproducing device on a recording medium or is reproduced from a recording medium is explained.

[0004] Drawing 9 is a flow chart which shows the flow of signal processing at the time of record. In processing step ST20 the analog video signal photoed with the video camera 2 is inputted into the digital image recording and reproducing device 1 and is changed into the digital video data of 4:2:2 by the video decoder 3. It is compressed into JPEG data by the JPEG compression extension means 4 in the following processing step ST21. In processing step ST22 JPEG data is once stored in the buffer memory 6 through the data bus 5 and the header which contained the time date code etc. in the buffer memory 6 is added to JPEG data. Furthermore in processing step ST23 the JPEG data in which the header was added is recorded on the archive medium 7 through the data bus 5.

[0005] Drawing 10 is a flow chart which shows the flow of signal processing at the time of reproduction and the JPEG data recorded on the archive medium 7 is once stored in the buffer memory 6 by control of CPU 5 in processing step ST30. Next in processing step ST31 header information is extracted and this generates the data of a time stamp etc. In processing step ST32 JPEG data is sent to the JPEG compression extension means 4 through the data bus 5 and is elongated by 4:2:2 digital video data. Finally in processing step ST33 the elongated 4:2:2 digital video data are changed into an NTSC analog signal with the video encoder 9 and a reproduced image is displayed with the monitor TV 10.

[0006]

[Problem(s) to be Solved by the Invention] The above-mentioned digital image recording and reproducing devices 1 are means of transportations such as a railroad and an airport and financial institutions such as a bank as a possible digital time lapse recorder of intermittent recording or are widely used for scientific research use such as a chemical experiment and observation of animals and plants. In order to analyze the recorded picture image data there the device provided with the SCSI interface which outputs outside the data by which JPEG compression was carried out on the occasion of recording the RS232C terminal is used. Compressed data can be sent to a personal computer etc. and it can change into the usual image data by carrying out JPEG extension with this personal computer. Therefore the recorded picture image data can correct adjustment and edge enhancement of contrast partial expansion etc. using the image-processing software of a computer etc. and after that JPEG compression is carried out again and it can also be saved.

[0007] However when the corrected picture image data was recorded on the same digital image recording and reproducing device 1 there was a possibility that which might not understand anymore whether it is data after which correcting by the original record data.

[0008] Since it was possible for a third party with bad faith to process the original record data in a similar way or to change for other data it was not able to detect easily

that a part of such image data was changed. Even if whether you are whom changes the picture image data which can serve as proof recorded by the above-mentioned digital image recording and reproducing device 1 such as a crime or a partial addition, deletion etc. are performed to the picture image data used as a criminal proof, this means that change of data is undetectable from the data itself. For this reason, about the weight of the evidence of the digital video data, it was not considered that it was sufficient for proving a crime etc.

[0009] In order to check whether they are original data, there is a method adapting encoding technology. However, when it is going to apply such a method to dynamic image data, there is a problem which huge and complicated calculation is needed and becomes what has high cost. Adding to picture image data by using as check data checksum (Checksum) used as the simple check method in order to inspect existence of an error is also considered. However, since it will be decoded easily and also the amount of data processing of add [in the case of dynamic image data / a checksum] increased, the check data added by addition also had the problem that it was necessary to provide hardware for exclusive use.

[0010] It is for this invention solving the above problems and aims at providing the digital data record / playback equipment which can detect easily whether it is that by which the digital data currently recorded on the medium was changed.

[0011] It can be detected easily whether the image data currently recorded on the recording medium is changed and the check code generation method with which a decipherment is moreover hard to be carried out is provided.

[0012]

[Means for Solving the Problem] A digital data recording device concerning claim 1 In a digital data recording device which records digital data on a recording medium, A data compression means which compresses digital data and an extraction means to extract some data from compressed digital data based on the 1st code function. It has a creating means which generates a check code based on the 2nd code function by making extracted data into a variable and an addition means added to a prescribed position of digital data which had a check code compressed.

[0013] In a digital data recording device concerning claim 2, the 2nd code function makes a variable a password which made a sampling number a variable.

[0014] Digital data is digital image data and a digital data recording device concerning claim 3 is provided with a JPEG compression means to compress this digital image data and adds a check code in a header of JPEG compression data.

[0015] Digital data playback equipment concerning claim 4 In digital data playback equipment which reproduces digital data compressed and recorded on a recording medium, The 1st extraction means that extracts some data from compression digital data based on the 1st code function. A creating means which generates the 1st check code based on the 2nd code function by making into a variable data extracted by the 1st extraction means. It has a comparison means to compare an extraction means with

the 2nd check code and 2nd check code that extracts the 2nd check code added to compression digital data and an extension means which elongates compression digital data. [1st]

[0016] Digital data playback equipment concerning claim 5 In digital data playback equipment which reproduces digital data compressed and recorded on a recording medium The 1st extraction means that extracts some data from compression digital data based on the 1st code function It has a calculating means which calculates data extracted by the 2nd extraction means that extracts a check code added to compression digital data and the 1st extraction means and a check code based on the 3rd code function and an extension means which elongates compression digital data.

[0017] Digital data is digital image data and digital data playback equipment concerning claim 6 is provided with a JPEG extension means which elongates compressed digital image data and extracts a check code from a header of JPEG compression data.

[0018] A check code generation method concerning claim 7 A digital data recording device Or it is a generation method of a check code used for digital data playback equipment A check code is generated by making a password which extracted two or more sampling data out of compressed digital data and made a variable extracted sampling data and its sampling number into a variable.

[0019] In a check code generation method concerning claim 8 a password which made a sampling number a variable is generated based on a code function.

[0020] A check code is generated in a check code generation method concerning claim 9 by arithmetic addition function which makes extracted sampling data and a password a variable.

[0021] A check code is generated in a check code generation method concerning claim 10 by addition on the Galois field which makes extracted sampling data and a password a variable.

[0022] A check code is generated in a check code generation method concerning claim 11 by EXCLUSIVE OR operation which makes extracted sampling data and a password a variable.

[0023] In a check code generation method concerning claim 12 sampling data are extracted based on a code function out of compressed digital data.

[0024]

[Embodiment of the Invention] Embodiment 1. drawing 1 is a block diagram showing the composition of the digital image recording and reproducing device in this embodiment of the invention 1. The same numerals are attached to the drawing (drawing 8) in which a conventional example corresponds and the corresponding portion.

[0025] The video camera by which 1 was connected to the digital image recording and reproducing device and 2 was connected to the digital image recording and reproducing device 1 in the figure The video decoder from which 3 changes the analog video signal from the video camera 2 into the digital video data of 4:2:2 profiles 4 receives a JPEG compression extension means 12 receives JPEG compression

data and a peculiar check code is added. The check code addition analyzer to analyze CPU by which 5 controls this digital image recording and reproducing device 1. The buffer memory used for temporary storing etc. of the JPEG data which 51 was connected to the data bus of CPU 5 and 6 was connected to the data bus 51 and was compressed by the JPEG compression extension means 4. Archive media such as HDD for 7 to save JPEG data, the video encoder from which 9 changes the digital video data of 4:2:2 profiles into an NTSC analog signal, and 10 are the monitor TVs connected to the digital image recording and reproducing device 1.

[0026] Drawing 2 is a flow chart which shows the flow of signal processing at the time of record and processing step STs 20–23 correspond to each processing of drawing 9. The analog video signal photoed with the video camera 2 in processing step ST20 is inputted into the digital image recording and reproducing device 1 and is changed into the digital video data of 4:2:2 by the video decoder 3. Next, it is compressed into JPEG data by the JPEG compression extension means 4 in processing step ST21. A predetermined check code is generated by the operation according [the JPEG data sampled in processing step ST40 / on processing step ST41 and] to the check code addition analyzer 12. This check code is once stored in the buffer memory 6 through the data bus 51 with the JPEG data compressed by processing step ST21.

[0027] Next, the generation method of the check code in processing step ST41 is described. First, in processing step ST40, as 1 byte each of sampling data ten points ($n=0-9$) are chosen for example, and 1 byte each of sampling data $S(n)$ are extracted based on the 1st code function (1) for example, the following formulas out of JPEG data $D(i)$.

[0028]

$$S(n) = D(axn + b) \quad \text{--- (1)}$$

However, a and b are constants.

[0029] In processing step ST41, based on the code function ($F(*)$): the code function of two shown in a following formula (2), it calculates by making these sampling-data $S(0) - S(9)$ into a variable, and the check code $C(n)$ is generated.

[0030]

$$C(n) = F(S(n)X(n)) \quad \text{--- (2)}$$

$X(n)$ is a code function for determining password arrangement.

[0031] It is for the others making the rule of a check code be hard to be analyzed as for this operation of $F(*)$. If the code function $X(n)$ which determines not only code function $F(*)$ but this password arrangement made secret, and the above-mentioned constants a and b are made secret, the analysis of check code $C(n)$ will become very difficult.

[0032] Drawing 4 is a figure showing the generation method of a check code typically. In a figure, the JPEG data in which 610 was compressed, the header data in which 620 contained the time date code of the head etc., and 621 are the check codes added in the header.

[0033] If the check code $C(n)$ of a formula (2) is rewritten when the secret function $F(*)$ is set to $X(n) = n$ which determines arithmetic addition and password arrangement as an example of the check code generated it will become the following formula (3) and the arrangement of a check code will become like drawing 5.

[0034]

$$C(n) = S(n) + n \quad (3)$$

However n is 0–9 in a sampling number.

[0035] By processing step ST42 the header data 620 having contained this check code 621 a time date code etc. are generated and it adds to the above-mentioned JrhoEG data 610 by processing step ST22. These header data 620 comprise a form based on a JPEG standard. In processing step ST23 the JPEG data 610 in which these header data 620 were added is recorded on the archive medium 7 through the data bus 51.

[0036] Next the operation at the time of reproduction is explained. Drawing 3 is a flow chart which shows the flow of signal processing at the time of reproduction and processing step STs 30–33 correspond to each processing of drawing 10.

[0037] The JPEG data currently recorded on the archive medium 7 in processing step ST30 is once stored in the buffer memory 6 by control of CPU 5. Header information is extracted from the JPEG data stored in this buffer memory 6 by processing step ST31 and a check code is further extracted from a header by processing step ST43.

[0038] In parallel to processing step STs 31 and 43 a check code is generated by the same method as the time of record from the JPEG data stored in the buffer memory 6 in processing step ST40. That is it asks for the same sampling data $S(n)$ of ten points ($n = 0-9$) as the time of record out of JPEG data $D(i)$ by the above-mentioned formula (1). In processing step ST41 the operation shown in the above-mentioned formula (3) at the sampling data $S(n)$ of ten points is performed and the check code $C(n)$ is generated. Although the operation of this processing step ST41 is the same processing as the operation for asking for the check code performed at the time of record and it becomes the same thing as the check code usually extracted by processing step ST43 When change of data is performed after record it asks as a different check code.

[0039] Then in processing step ST45 the check code extracted by processing step ST43 is compared with the check code computed by processing step ST41. When two check codes differ mutually since change of data is performed after record it orders so that an alarm display may be taken out to the monitor TV 10 by processing step ST46. Once the reproduced picture image data is stored in the archive medium 7 by this the warning of a purport which was able to add change depending on whether you are whom is made.

[0040] In processing step ST32 JPEG data is sent to the JPEG compression extension means 4 through the data bus 51 and is again elongated by the digital video data. In processing step ST33 with the video encoder 9 this elongated digital video data is changed into an NTSC analog signal and displays a reproduced image on the monitor

TV 10. The warning ordered by processing step ST46 is displayed in piles on the reproduced image at this time and specifies that it is the altered data. In this way the picture image data under reproduction can show clearly that it is altered by whether you are whom.

[0041] As mentioned above, since some compressed JPEG data is sampled, a check code is generated and it was made to store in the archive medium 7 with a digital video data. It is easily detectable whether it is that by which the digital data currently recorded by the throughput of very little data was changed.

[0042] Next, the picture image data in which it was recorded whether you are whom is once changed into the usual image data by carrying out JPEG extension. After changing a part of image data using the image-processing software of a computer etc., after that a case so that JPEG compression may be carried out again and it may change for the original record data is considered. Even if the range which changed picture image data is only the field where some picture image data was restricted. In JPEG data after being compressed by the DCT encoding performed in process of JPEG compression processing or Huffman encoding, it will spread throughout the JPEG data after the influence of the original picture image data twisted to change in part compressing. For this reason, even if it only uses few about ten sample takeoff points, change of picture image data is certainly detectable.

[0043] It is also next to impossible to make it not know that the check code was newly attached and changed to the changed picture image data. Because the arithmetic method of the sampling rule from picture image data or a check code shown by the formula (1) and the formula (2) is a thing based on a code function. Unless all code functions including the code function for determining password arrangement are known, it is because it is very difficult for a third party to analyze the check code itself. Therefore, also when the digital image recording and reproducing device of this Embodiment 1 heightens the weight of the evidence of picture image data, it is effective.

[0044] As stated above, the generation method of the check code for detecting change of the digital image in the digital data recording and reproducing device of Embodiment 1 has high reliability also to the analysis by very high ability to detect and a third party with bad faith, though it is a simple method. For this reason, when a crime etc. occurs, the picture image data recorded with the digital data recording device of this embodiment has high weight of the evidence.

[0045] A check code is storing in the intact reserved area of the header data which carried out JPEG compression, and it is possible to reproduce even if it is a digital data recording and reproducing device without the function to add and analyze the usual check code.

[0046] This may be other functions although the usual arithmetic addition as shown in a formula (2) was used in the embodiment 2. embodiment 1 as code function [at the time of generating the check code C] F (*). For example, a check code is also

generable using the addition operation of the Galois field (finite field) etc.

[0047] Since the usual arithmetic addition is performed [Embodiment 1] to 8-bit data when beam going up occurs in an added result by 8-bit data omission of a beam [**** and others] going-up portion is performed for the result of an operation. For this reason although the same check code will be generated to different sampling data if it does so change of picture image data may be overlooked. Then by using the addition on the Galois field instead of usual arithmetic addition like a formula (2) as code function $F(*)$ if sampling data differs a certainly different check code will be generated. By this a possibility of overlooking change of picture image data can be made small.

[0048] In the embodiment 3. embodiment 1 when generating the check code $C(n)$ the usual arithmetic addition was used as code function $F(*)$ as shown in a formula (2) but this may be other functions for example may use EXCLUSIVE OR operation. As shown in drawing 6 EXCLUSIVE OR operation is performed between header data (higher rank) the password arrangement $X(10)$ and header data (low rank) the password arrangement $X(11)$ sampling-data $S(0)$ the password arrangement $X(0)$ etc. According to such an operation like Embodiment 2 if sampling data differs a certainly different check code is generable.

[0049] This method has an effect which can generate a check code more easily than the method of using addition of the Galois field used by Embodiment 2.

[0050] As shown in drawing 6 apart from header data the version information of a code function can be added to a check code and the code function for determining the sampling rule from picture image data the arithmetic method of a check code and password arrangement according to this version information can also be changed. Here version information is information which specifies two or more versions (Ver.1.0 Ver.2.0 grade) which memorize a code function different respectively and the version information of the code function used for every device or every recording periods is added to a check code.

[0051] Even when carrying out like this and the code function of a certain version is known by the third party with bad faith the reliability of the check code generated with the code function of the other version can be maintained and it is effective in the ability to prevent change of image data.

[0052] The header 620 shown in drawing 4 is divided into the portion (upper portion) before the check code 621 in which it is inserted for example and a back portion (bottom part) the header of an upper portion is added it is considered as the header data of a higher rank the header of a bottom part is added and it is considered as low-ranking header data. The header data of these higher ranks and a low rank and EXCLUSIVE OR operation of the password arrangement $X(10)$ and $X(11)$ are performed and it adds to the check code generated from sampling data. By using such a check code also when the header information itself is changed it can be detected. Since information with date information a camera number besides information required

for extension of JPEG data etc. important for a header part is recorded a still more reliable device can be obtained by forming the detection means of change of such a header part.

[0053] In the embodiment 4 embodiments 1-3 as shown in a formula (2) as secret function $F(*)$ computed one check code using one sampling data and one password but. As shown in the following formulas (4) one check code may be computed using two or more sampling data and two or more passwords.

[0054]

$$C(n) = F(S(n)S(n+1)X(n)X(n+1)) \quad \text{--- (4)}$$

In this case analysis of the check code by a third party with bad faith is made much more difficult and it is effective in raising the reliability of a check code.

[0055] Although the constants a and b beforehand decided by the linear expression showing in a formula (1) were used in the embodiment 5. embodiment 1 it may be made to change the constants a and b according to data volume so that several n of a sample takeoff point may not change even if the data volume of JPEG data changes.

[0056] For example if N is determined like a total data number $a = N/16$ and $b = 2$ it will be $S(n) = D(N+2)(n/16)$. --- (5)

Ten points can be sampled from the 3rd data of a next door and the data divided into 16. Since the number of sample takeoff points will not change if it carries out like this even when JPEG data is small it is effective in the accuracy of change detection not becoming low. Since a sample takeoff point can be easily changed with the data volume of JPEG data analysis of the check code by a third party with bad faith is made much more difficult and it is effective in raising the reliability of a check code.

[0057] Although the linear expression showing in a formula (1) was used as a method of sampling the sampling data $S(n)$ in the embodiment 6. embodiment 1 it may sample by other methods. For example other functions such as logarithm and trigonometric functions are the example. A sampling position may be changed using the method of sampling using a random number and a secret password. In this case analysis of the check code by a third party with bad faith is made much more difficult and it is effective in raising the reliability of a check code.

[0058] Embodiment 7. drawing 7 is a flow chart which shows the flow of signal processing at the time of the reproduction in this embodiment of the invention 7 and processing step STs 30-33 correspond to each processing of drawing 10.

[0059] The JPEG data currently recorded on the archive medium 7 in processing step ST30 is once stored in the buffer memory 6 by control of CPU5. Header information is extracted from the JPEG data stored in this buffer memory 6 by processing step ST31 and a check code is further extracted from a header by processing step ST43.

[0060] In parallel to processing step STs 31 and 43 it asks for the sampling data $S(n)$ by a formula (1) from the JPEG data stored in this buffer memory 6 by processing step ST40. In processing step ST47 these sampling-data $S(n)$ and the check code extracted by processing step ST43 calculate directly and the check of being the

changed data is performed.

[0061]the case where the check code at the time of record is generated by the formula (3) as an operation in processing step ST47for example -- $V(n) = S(n) - C(n) + n$ -- (6)

** -- if the operation [like] is set upthe existence of change can be judged by whether it is result-of-an-operation $V(n) = 0$ in processing step ST48.

[0062]Thereforeif it is $V(n) \neq 0$ in processing step ST48it will become possible to tell ordering so that an alarm display may be taken out to the monitor TV 10 by processing step ST46and being changed by whether you are whom.

[0063]In the above-mentioned Embodiments 1-7although each uses JPEG compression as a compression method of image dataMrhoepsilonG1MPEG 2MPEG4H.261etc. are effective similarly to the picture image data based on other compression methods.

[0064]It can apply also to the usual continuous recording device in addition to the digital time lapse recorder which performs intermittent recording as a recorderand the same effect is done so.

[0065]Although the above-mentioned Embodiments 1-7 explained record of image datathe same effect is done so even if it carries out record reproduction of the data of other kinds of voice data etc.for example.

[0066]Although the circuit for exclusive use is established in the addition analyzer 12 of the check code in the above-mentioned Embodiments 1-7since these processings can be performed very simpleit is also possible to simplify hardware by CPU5as it performs by software.

[0067]

[Effect of the Invention]Since this invention is constituted as explained aboveit does an effect as taken below so.

[0068]According to the digital data recording device indicated to claim 1it is easily detectable whether it is that by which the digital data currently recorded on the medium was changed.

[0069]In the device of claim 2since the password which made the sampling number the variable is made into a variablewhen the analysis of a check code becomes very difficult and heightens the weight of the evidence of picture image datait is effective.

[of the 2nd code function]

[0070]Since it had a JPEG compression means to compress this digital image data and the check code was added in the header of JPEG compression data in the device of claim 3 when digital data was digital image dataChange of a digital image can be detected by a simple methodand change of a third party with bad faith can be prevented with high reliability.

[0071]According to the digital data playback equipment indicated to claim 4it is easily detectable whether it is that by which the digital data currently reproduced was changed.

[0072]According to the digital data playback equipment indicated to claim 5 it is easily detectable whether it is that by which the digital data currently reproduced only by the easy operation was changed.

[0073]Since it had the JPEG extension means which elongates the compressed digital image data and the check code was extracted from the header of JPEG compression data in the device of claim 6 when digital data was digital image data Change of a digital image can be detected by a simple method and change of a third party with bad faith can be prevented with high reliability.

[0074]According to the generation method of the check code indicated to claim 7 it can be detected easily whether the image data currently recorded on the recording medium is changed and the check code a decipherment is moreover hard to be made can be generated.

[0075]Since it is generated based on the code function the analysis of a check code has it when the password which made the sampling number the variable in the method of claim 8 becomes very difficult and heightens the weight of the evidence of picture image data. [effective]

[0076]In the method of claim 9 since the check code is generated by the arithmetic addition function which makes the extracted sampling data and a password a variable change of picture image data can detect certainly only by using few sample takeoff points.

[0077]Since the check code is generated in the method of claim 10 by the addition on the Galois field which makes the extracted sampling data and a password a variable If sampling data differs a certainly different check code will be generated and a possibility of overlooking change of picture image data can be made small.

[0078]In the method of claim 11 since the check code is generated by the EXCLUSIVE OR operation which makes the extracted sampling data and a password a variable a check code is easily generable.

[0079]In the method of claim 12 since sampling data are extracted based on the code function out of the compressed digital data the check code a decipherment is hard to be made is generable.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is a block diagram showing the composition of the digital image recording and reproducing device concerning this embodiment of the invention 1.

[Drawing 2] It is a flow chart which shows the recording operation concerning this embodiment of the invention 1.

[Drawing 3] It is a flow chart which shows the reproduction motion concerning this embodiment of the invention 1.

[Drawing 4] It is a figure showing typically generation of the check code concerning this embodiment of the invention 1.

[Drawing 5] It is a figure showing the check code concerning this embodiment of the invention 1.

[Drawing 6] It is a figure showing the check code concerning this embodiment of the invention 3.

[Drawing 7] It is a flow chart which shows the reproduction motion concerning this embodiment of the invention 7.

[Drawing 8] It is a block diagram showing the composition of the conventional digital image recording and reproducing device.

[Drawing 9] It is a flow chart which shows the recording operation of the conventional digital image recording and reproducing device.

[Drawing 10] It is a flow chart which shows the reproduction motion of the conventional digital image recording and reproducing device.

[Description of Notations]

1 A digital image recording and reproducing device and 2 A video camera and 3 Video decoder 4 A JPEG compression extension means 5 CPU and 6 A buffer memory 7 archive media 8 communication interfaces 9 video encoder 10 monitor TV and 12 A check code addition analyzer and 51 Data bus.
